Créer un compte Se connecter

Article Discussion Lire Modifier le code Afficher l'historique Rechercher

WIKIPÉDIA
L'encyclopédie libre

Navigation
Accueil
Portails thématiques
Article au hasard
Contact

Contribuer
Débuter sur Wikipédia
Aide
Communauté
Modifications récentes
Faire un don

Imprimer / exporter
Créer un livre
Télécharger comme PDF
Version imprimable

Outils
Pages liées
Suivi des pages liées
Importer un fichier
Pages spéciales
Adresse de cette version
Information sur la page
Élément sur Wikidata
Citer cette page

Autres langues
Deutsch
English
Esperanto
Español
Suomi
Italiano
日本語
Bahasa Melayu
Nederlands
Português
Русский
中文
Modifier les liens

Serveur racine du DNS

Un **serveur racine du DNS** est un serveur DNS qui répond aux requêtes qui concernent les noms de domaine de premier niveau (top-level domain, TLD) et qui les redirige vers le serveur DNS de premier niveau concerné. Bien qu'il puisse exister d'autres hiérarchies DNS avec d'autres serveurs racine, « serveur racine du DNS » est généralement utilisé pour désigner l'un des treize serveurs racine du *Domain Name System* d'Internet géré sous l'autorité de l'ICANN.

Dans le système des noms de domaine, le point est un séparateur de domaine. Par convention, un Fully qualified domain name est terminé par un point, ce qui signifie qu'il est suivi par une chaîne vide qui représente le domaine racine. Par extension, on représente aussi le domaine racine par un point.

Les domaines de premier niveau (par exemple .com, .org et .fr) sont des sous-domaines du domaine racine.

Sommaire

1 Requêtes DNS destinées aux serveurs racine
2 Les serveurs racine du DNS
3 Limitation du nombre de serveurs
4 Sécurité des serveurs racine
4.1 Attaque de 2002
4.2 Attaque de 2007
5 Zone racine
6 Hiérarchies alternatives
6.1 Hiérarchies alternatives en pair à pair
7 Notes et références
8 Voir aussi
8.1 Articles connexes
8.2 Liens externes

Requêtes DNS destinées aux serveurs racine [modifier le code]

Un serveur DNS s'adresse à un serveur racine dans deux cas :

- au démarrage, pour obtenir la liste à jour des serveurs racine.
- quand il doit déterminer la liste des serveurs de noms d'un domaine de premier niveau.

Les informations sont ensuite mises dans le cache du serveur DNS pendant une longue durée : 6 jours pour la liste des serveurs racine, 2 jours pour les informations des serveurs des TLD. Ces informations variant peu, les requêtes vers les serveurs racine sont donc relativement peu nombreuses.

Les serveurs racine sont non-récursifs, c'est-à-dire qu'ils ne fournissent que des réponses qui font autorité, ne transmettent aucune requête à un autre serveur et ne font pas usage d'un cache. Ils ne sont donc pas utilisables directement par un *resolver* d'un client final.

Une étude de 2003[1] indique que seuls 2 % des requêtes à destination de ces serveurs étaient légitimes. Les mises en cache incorrectes ou inexistantes sont à l'origine de 75 % des demandes. 12,5 % concernent des demandes pour des domaines de premier niveau inconnus, 7 % parce qu'elles traitent des adresses IP comme des noms de domaines, etc. Certains ordinateurs de bureau mal configurés tentent même de mettre à jour les enregistrements des serveurs racine ou sollicitent de la récursion, ce qui est le résultat d'une erreur de configuration. Les problèmes observés et les solutions pour y remédier sont décrites dans la RFC 4697 .

En 2007, il y avait environ dix milliards de requêtes vers les serveurs racine quotidiennement[2].

Les serveurs racine font également autorité pour le domaine de premier niveau .arpa. La zone in-addr.arpa, utilisée pour la résolution inverse des adresses IPv4, était gérée par les serveurs racine jusqu'en février 2011. Elle est désormais sous la gestion technique des registres Internet régionaux[3].

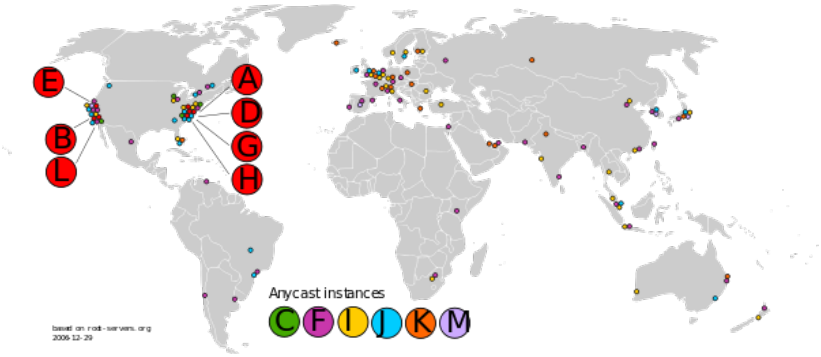
Les serveurs racine du DNS [modifier le code]

Il y a apparemment 13 serveurs racine du DNS[4] dont les noms sont de la forme `lettre.root-servers.net` (la liste est disponible sur root-servers.org) où `lettre` est une lettre comprise entre A et M. Douze organisations[2] contrôlent ces serveurs, deux sont européennes (RIPE NCC et Autonomica), une japonaise (WIDE), les autres étant américaines. Neuf de ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers, il y a ainsi plus de 130 sites dans 53 pays qui hébergent un serveur racine du DNS[5,2].

Les serveurs ont été regroupés sous le même nom de domaine pour exploiter un mécanisme d'évitement de répétition des noms dans le protocole DNS.

Lettre	adresse IPv4[6]	adresse IPv6[6]	Autonomous System[6]	Ancien nom	Société	Localisation	Sites (global/local)[6]	Logiciel
A	198.41.0.4	2001:503:ba3e::2:30	AS19836	ns.internic.net	VeriSign	trafic distribué par	6 (6/0)	BIND

						anycast	(6/0)	
B	192.228.79.201[7]	2001:478:65::53 (pas encore dans la zone)	AS4	ns1.isi.edu	USC-ISI (en)	Marina Del Rey, Californie, États-Unis	1 (1/0)	BIND
C	192.33.4.12	2001:500:2::c (pas encore dans la zone)	AS2149	c.psi.net	Cogent Communications	trafic distribué par anycast	6 (6/0)	BIND
D	199.7.91.13[8]	2001:500:2d::d	AS27	terp.umd.edu	Université du Maryland	College Park, Maryland, États-Unis	1 (1/0)	BIND
E	192.203.230.10		AS297	ns.nasa.gov	NASA	Mountain View, Californie, États-Unis	1 (1/0)	BIND
F	192.5.5.241	2001:500:2f::f	AS3557	ns.isc.org	Internet Systems Consortium	trafic distribué par anycast	49 (2/47)	BIND 9[9]
« G » (Archive • Wikiwix • Archive.is • Google • Que faire ?). Consulté le 2013-04-08	192.112.36.4		AS5927	ns.nic.ddn.mil	Defense Information Systems Agency (en)	trafic distribué par anycast	6 (6/0)	BIND
H	128.63.2.53	2001:500:1::803f:235	AS13	aos.arl.army.mil	United States Army Research Laboratory (en)	Aberdeen, Maryland, États-Unis	1 (1/0)	NSD
I	192.36.148.17	2001:7fe::53	AS29216	nic.nordu.net	Autonomica	trafic distribué par anycast	36	BIND
J	192.58.128.30[10]	2001:503:c27::2:30	AS26415		VeriSign	trafic distribué par anycast	70 (63/7)	BIND
K	193.0.14.129	2001:7fd::1	AS25152		RIPE NCC	trafic distribué par anycast	18 (5/13)	NSD[11]
L	199.7.83.42[12]	2001:500:3::42	AS20144		ICANN	trafic distribué par anycast	38 (37/1)	NSD[13]
M	202.12.27.33	2001:dc3::35	AS7500		WIDE Project	trafic distribué par anycast	6 (5/1)	BIND



Limitation du nombre de serveurs [modifier le code]

La RFC 1035 prévoit que les requêtes et les réponses DNS sur UDP ne dépassent pas 512 octets. Si la réponse est plus volumineuse, TCP doit alors être utilisé. Ceci consomme plus de ressources et présente le risque d'être bloqué par un pare-feu. Ce cas de réponse volumineuse est rare en pratique, mais la liste des serveurs de noms de la zone racine avec les adresses IP correspondantes atteint cette limite, 671 octets étant nécessaires pour une

réponse complète en juillet 2010.

Les serveurs A, C, F, G, I, J, K, L et M sont maintenant distribués géographiquement grâce à anycast. En général, le serveur le plus proche du client au sens du réseau sera alors utilisé. C'est ainsi que la plupart des serveurs DNS physiques sont à présent situés hors des États-Unis.

Les serveurs racines du DNS peuvent également être déclinés localement, sur les réseaux des FAI par exemple. Ils doivent être synchronisés avec le fichier de la zone racine[14] du Département du Commerce des États-Unis ainsi que le préconise l'ICANN. De tels serveurs ne sont pas des serveurs DNS alternatifs mais une déclinaison locale des serveurs racines du DNS A à M.

L'extension EDNS0 (RFC 2671) permet d'utiliser une taille de paquets plus élevée, sa prise en charge est recommandée pour IPv6 comme pour DNSSEC.

Sécurité des serveurs racine [modifier le code]

Les serveurs racine jouent un rôle important dans le système DNS. Si l'un ou quelques-uns d'entre eux ne répondent plus, la charge est répartie entre les serveurs qui subsistent. Si aucun d'entre eux ne pouvait répondre aux requêtes, les noms de domaines deviendraient progressivement inaccessibles, au fur et à mesure que les informations dans les caches parviendraient à expiration, c'est-à-dire environ 2 % par heure d'indisponibilité totale[15].

La possibilité d'un bug qui affecterait l'ensemble des serveurs est limitée par la diversité des versions logicielles employées : BINDv8, BINDv9 et NSD. Le matériel sur lequel fonctionnent les serveurs est divers.

Les risques d'attaques par déni de service sont mitigés par le nombre de serveurs en anycast. L'adresse unicast de la plupart des serveurs n'est pas publiée pour éviter les attaques ciblées. Il n'est pas rare que l'un des serveurs fasse l'objet d'une attaque par déni de service, sans que cela affecte de façon perceptible la qualité du fonctionnement du DNS dans son ensemble.

Certaines attaques de grande ampleur ont cependant eu lieu au xxie siècle :

Attaque de 2002 [modifier le code]

Le 21 octobre 2002, la racine complète du DNS a fait l'objet d'une attaque de grande ampleur pendant une heure, les 13 serveurs A à M étant visés[16, 17]. Pendant cette attaque, 7 serveurs sur 13 ont vu leur performances dégradées en raison d'un flux de 100 000 à 200 000 requêtes par seconde vers chacun des serveurs. Toutefois, l'attaque n'a pas provoqué de grandes perturbations du réseau mondial, ce qui montre la robustesse du système. Selon le PDG de Verisign, qui gère deux serveurs racine, l'ensemble des requêtes aurait pu être assuré par un seul serveur.

L'attaque a été réalisée selon la méthode DDoS (déni de service). Les pirates ont pu, grâce à un parc de machines très important, générer un nombre de requêtes deux à trois fois supérieur à la capacité de charge des treize serveurs visés, soit quarante fois le volume habituel des requêtes.

Le système anycast a été mis en place après cette attaque pour neutraliser les attaques de type DoS.

Attaque de 2007 [modifier le code]

Le 6 février 2007, les serveurs F, G, L et M ont été attaqués pendant 24 heures à partir de 10:00 UTC[18]. G et L ont été affectés sérieusement, tandis que F et M ont rapporté une charge inhabituelle. L'impact sur M a été amoindri grâce à anycast.

La source s'avère être un réseau botnet de 5000 machines essentiellement basé en Corée du Sud et dirigé depuis les États-Unis[19].

Zone racine [modifier le code]

Le fichier de la zone racine est disponible publiquement[20]. Il est peu volumineux (de l'ordre de 200 Ko) et contient 283 délégations de domaines de premier niveau, 1145 serveurs de noms, 1124 A records et 251 AAAA records en juillet 2010.

Des signatures DNSSEC RRSIG ont été ajoutés aux fichiers de la racine en juillet 2010[21].

Hiérarchies alternatives [modifier le code]

Il est possible de créer une hiérarchie DNS alternative avec un autre ensemble de serveurs racine. Un serveur qui voudrait y avoir recours doit disposer de la liste des serveurs racine de cette hiérarchie DNS alternative.

Ces hiérarchies peuvent définir d'autres domaines de premier niveau. Ces domaines ne seront pas accessibles par les clients qui n'utilisent pas cet ensemble de serveurs. La possibilité qu'un domaine de premier niveau soit défini de façon différente entre des hiérarchies alternatives existe également.

Parmi ces hiérarchies alternatives, on peut citer :

- OpenNIC,
- Unifiedroot,
- AlterNIC (en), qui a cessé ses activités en 1997,
- eDNS, clos en 1998.

L'Internet Architecture Board (IAB) a exprimé, dans le RFC 2826 , la nécessité de conserver une hiérarchie unique pour préserver la cohésion du réseau Internet.

Hiérarchies alternatives en pair à pair [modifier le code]

Différents systèmes de réseaux en pair à pair ont également été créés, dans le but d'offrir une alternative viable tout en réduisant les frais de l'infrastructure, parmi lesquels :

- CoDoNS, développé à l'université Cornell[22]
- GNU Name System (ou GNS), utilisé par le réseau GNUnet avec le TLD `.gnu`[23]
- Kadnode, basé sur le protocole en table de hachage distribuée Kademlia[24]
- Namecoin, basé sur Bitcoin, utilise le TLD `.bit`[25]
- OddDNS[26] (arrêté en 2012)[27].

Notes et références [modifier le code]

1. ↑ [PDF] *Wow, That's a Lot of Packets* , Duane Wessels
2. ↑ a, b et c ISOC
3. ↑ in-addr.arpa transition
4. ↑ ftp://rs.internic.net/domain/named.cache
5. ↑ There are not 13 root servers , Kim Davies, novembre 2007
6. ↑ a, b, c et d AS et adresse IPv4/v6 de Root-servers.org homepage visité le 15 novembre 2010
7. ↑ depuis janvier 2004, était 128.9.0.107 autrefois (en) « New IPv4 address for b.root-servers.net »
8. ↑ L'adresse IP était 128.8.10.90 jusqu'en janvier 2013 D-Root is Changing its IPv4 Address on 3 January 2013
9. ↑ F-root | Internet Systems Consortium
10. ↑ depuis ovember 2002, était 198.41.0.10 autrefois
11. ↑ K-root Homepage
12. ↑ depuis novembre 207, était 198.32.64.12 autrefois (en) « Advisory — "L Root" changing IP address on 1st November » , ICANN
13. ↑ l.root-servers.net
14. ↑ ftp://rs.internic.net/domain/
15. ↑ cf ISOC, le TTL des délégations TLD étant de deux jours
16. ↑ Nameserver DoS Attack October 2002 , CAIDA
17. ↑ Events of October 21 , Paul Vixie
18. ↑ « =Factsheet - Root server attack on 6 February 2007 » (Archive • Wikiwix • Archive.is • Google • Que faire ?)
19. ↑ Root DDoS Attack Analysis
20. ↑ http://www.internic.net/domain/
21. ↑ ISC Praises Momentous Step Forward in Securing the Domain Name System , ISC, 15 juillet 2010
22. ↑ http://www.cs.cornell.edu/people/egs/beehive/codons.php
23. ↑ https://gnunet.org/book/export/html/1677
24. ↑ https://github.com/mwarning/kadnode
25. ↑ [1]
26. ↑ http://www.pcinpact.com/news/70085-oddns-filtrage-dns-p2p.htm
27. ↑ https://gnunet.org/comment/841#comment-841

Voir aussi [modifier le code]

Articles connexes [modifier le code]

- Anycast
- Empoisonnement du cache DNS
- IPv6

Liens externes [modifier le code]

- Root Server Technical Operations Association
- « DNS Root Server System Advisory Committee » (Archive • Wikiwix • Archive.is • Google • Que faire ?). Consulté le 2013-04-08
- Bogus Queries received at the Root Servers

Portail d'Internet

Catégories : Domain Name System | Serveur informatique

Dernière modification de cette page le 23 mars 2014 à 13:44.

Droit d'auteur : les textes sont disponibles sous licence Creative Commons paternité partage à l'identique ; d'autres conditions peuvent s'appliquer. Voyez les conditions d'utilisation pour plus de détails, ainsi que les crédits graphiques. En cas de réutilisation des textes de cette page, voyez comment citer les auteurs et mentionner la licence.
Wikipedia® est une marque déposée de la Wikimedia Foundation, Inc., organisation de bienfaisance régie par le paragraphe 501(c)(3) du code fiscal des États-Unis.

Politique de confidentialité À propos de Wikipédia Avertissements Développeurs Version mobile